10

Before the
Department of the Treasury
Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve
Federal Deposit Insurance Corporation
Office of Thrift Supervision
Washington, D.C.

In the Matter of	)	**OCC File No. 03-18**
	)	**BOG File No. OP-1155**
Notice Regarding Unauthorized	)	**OTS File No. 03-35**
Access to Customer Information	)	

COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER AND THE UNITED STATES PUBLIC INTEREST RESEARCH GROUP
October 14, 2003

Pursuant to the notice[1] published on August 12, 2003 regarding the proposed guidance entitled Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("proposed Guidance"), the Electronic Privacy Information Center submits the following comments. Security of personal information is an important fair information practice. Under the 1980 Organization for Economic Cooperation and Development articulation of fair information practices, the security safeguards principle requires data collectors to protect personal information from loss, unauthorized access, destruction, improper use, modification, or disclosure.[2] We applaud the joint efforts of the agencies to provide guidance on this important guideline.

I. General Comments

Section II of the proposed Guidance lists the components of a response program while section III provides circumstances for customer notice. EPIC strongly urges the Agencies to consider the following issues that relate to an effective response program that have not been raised in the proposed Guidance.

---

[1] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("proposed Guidance"), 68 Fed. Reg. 155, 47954.
[2] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), at http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

A. THE AGENCIES SHOULD REQUIRE FINANCIAL INSTITUTIONS TO INSTITUTE MONITORING SYSTEMS AS SECURITY MEASURE OF ITS INFORMATION SECURITY SYSTEM.

In accordance with the published Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Security Guidelines")[3] that establish the need for response programs, each bank could institute monitoring systems and procedures to "detect actual and attempted attacks on or intrusions into customer information systems."[4] Language of the Security Guidelines require banks to "consider" whether such a security measure is "appropriate for the bank and, if so, adopt" such measure. Security measures mentioned include the monitoring systems and response programs. By mandating such monitoring systems for a bank's information security program, rather than merely requiring a consideration of the issue, it will allow for superior facilitation of the assessment analysis component of the response program. Monitoring systems are an essential element necessary to maintain the integrity of the customer information systems and to be able to proceed with a comprehensive response program.

B. THE NOTIFICATION TO REGULATORY AGENCIES COMPONENT OF THE PROPOSED GUIDANCE'S IS DEFICIENT WITH REGARDS TO WHEN NOTICE SHOULD BE GIVEN AND THE CONTENT OF THE NOTICE.

Financial institutions must be held accountable for security events that are directed towards their customer information systems. The Agency notification component of the response program represents an important disclosure mechanism that is essential in establishing whether financial institutions have properly instituted the appropriate safeguard standards of the Gramm-Leach-Bliley Act ("GLBA") and the Security Guidelines. As this component of the response program is necessary, the proposed Guidance is deficient as to when the financial institutions should provide their primary Federal regulator with notice of a security event, and the content of such notice.

1. NOTIFICATION OF ALL SECURITY EVENTS TO FEDERAL REGULATORS IS CRITICAL.

The language used to establish the notification standard from the GLBA leaves room for immense interpretation as to when the financial institutions must notify their primary Federal regulator. "The institution should promptly notify its primary Federal regulator when it becomes aware of an incident involving *unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers*."[5] This standard should not be construed to withhold accountability for notification in cases where the unauthorized access is to the customer information systems generally, rather than only when customer information is accessed or used.

Under the Security Guidelines, an institution's customer information system consists of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information,

[3] 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D-2, and part 225, app. F (Board); 12 CFR part 364, app. B (FDIC); and 12 CFR part 570, app. B (OTS).
[4] Security Guidelines, Paragraph III(C)(1)(f).
[5] Gramm-Leach-Bliley Act (GLBA), Title V, Pub. L. No. 106-102, 113 Stat. 1436 (1999) (*codified at* 15 U.S.C. §§ 6801-6827 (2000), at § 6801(b)(3)).

including the systems maintained by its service providers.[6] The potential for substantial harm or inconvenience is present in every instance of unauthorized access to the customer information systems. Every unauthorized access to or manipulation of a customer information system's reliability can result in substantial harm or inconvenience, especially if such manipulation includes the introduction of a virus, worm, Trojan horse, or any other such deceptive or disruptive mechanism that can affect a system's integrity, confidentiality, or availability. And even if there is no apparent affect to the systems generally, the opportunity is great for misuse of the information gathered from the customer information systems in the commission of identity theft or to facilitate methods to gather additional information in the commission of an identity theft scheme, such as phishing.[7] In a survey conducted by the Federal Trade Commission the number of victims of identity theft in the United States for 2002 approached 10 million.[8] Many victims reported that they did not know how their personal information was compromised, but among those who did know, a significant percentage reported that a financial institution was responsible for the crime.[9] Clearly, individuals need more notice of security breaches so that they can proactively remedy the crime.

The proposed Guidance requires service providers to fully disclose to the institution information relating to any breach in security resulting in an unauthorized intrusion into the institution's customer information system maintained by a service provider.[10] This same disclosure standard should also apply to the financial institutions, with respect to the financial institution's notification obligation to their respective primary Federal regulator. Under the proposed Guidance, notification is made to the financial institution's primary Federal regulator only when the institution "becomes aware of an incident involving unauthorized access to or use of customer information that *could* result in substantial harm or inconvenience to its customers".[11] It is imperative that there be no room for ambiguous interpretation within the language here that triggers the notification provision to the appropriate Federal regulator. Therefore, notice should be furnished to an institution's primary Federal regulator in all security events affecting customer information systems.

---

[6] Security Guidelines, paragraph I(C)(2).

[7] Phishers first steal a company's identity then use it to victimize consumers by stealing their credit identities. *See* Consumer Financial Services Law Report, *Minor 'phishes' for private financial data,* Identity Theft; Vol. 7, No. 5 (August 13, 2003).

[8] The Federal Trade Commission (FTC)'s, *Identity Theft Survey Report* of September 2003, estimated that 4.6% of American adults were victims, is available at <http://www.ftc.gov/os/2003/09/synovatereport.pdf>.

[9] *Id.*

[10] Guidance, appendix, paragraph I.

[11] *Id.* at paragraph II(B).

2. SPECIFIC GUIDANCE AS TO THE METHOD AND CONTENT OF THE AGENCY NOTIFICATIONS IS NEEDED.

The proposed Guidance offers no leadership as to the method of notification by the financial institution to its primary Federal regulator when it becomes aware of such incidences. Under the scheme of the proposed Guidance, the notification component is a non-specific method of putting the Agencies on notice only that an incident of unauthorized access to customer information has occurred. There is no specification as to content of the notices to the Agencies and the different methods of notification that may be available to the institutions. The Agencies should develop a common standard of notification whereby they are given comprehensive details, in order to process such information for purposes such as formulating their own response to the incidents, regulate GLBA compliance of the financial institutions, and gather statistical data in preparation of summaries of such incidences. The statistical data could include the number of incidences reported annually and the number of times the incidences warranted customer notice.

3. THERE SHOULD BE A HIGHER ACCOUNTABILITY OF THE OFFICERS BY CERTIFYING THE ACCURACY OF THE NOTIFICATION DISCLOSURES AND COMPLIANCE OF THE GLBA.

As part of this notification standard, the Agencies should also include a certification requirement, in the spirit of the Sarbanes-Oxley Act of 2002. As the GLBA was passed by Congress to ensure that financial institution respect the privacy of its customers and protect the security and confidentiality of those customers' nonpublic personal information[12], the Sarbanes-Oxley Act of 2002 was passed to protect investors by improving the accuracy and reliability of corporate disclosures.[13] Sarbanes-Oxley's certification requirements contemplate a higher lever of involvement by senior management in the disclosure and reporting process of a company's filings. Under the Act, an officer must certify in each annual or quarterly report filed under the Act that: 1) the signing officer has reviewed the report; 2) the report does not contain any untrue statements of material fact or omit a material fact necessary not to make the report misleading; 3) the report fairly presents the [financial] condition and results of operations of the issuer as of the periods presented in the report; 4) the signing officer is responsible for establishing and maintaining internal controls; 5) the signing officer has disclosed all significant deficiencies in the design or operation of internal controls and any fraud that involves management or other employees who have a significant role in the internal controls; and 6) the signing officer indicates whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.[14]

A similar certification provision should be added to the required notification of the Agencies by the financial institutions whereby an officer of the institution, or someone designated by the board such as the director of the information security program, certifies that the financial

[12] 15 USC § 6801(a).
[13] Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act, Pub. L. No. 107-204, 116 Stat. 745 (2002).
[14] 15 USC § 7241(a).

institution is in compliance with the requirements of the GLBA, the Security Guidelines, and this Guidance.[15] Uncertified notices to the Agencies regarding incidents of unauthorized access to customer information have no teeth and do little more than put the Agencies on notice merely that an incident has occurred.

4. INFORMATION SHOULD BE MADE AVAILABLE BY THE AGENCIES ON THEIR WEB SITES.

Annual figures of the reported incidences should be made available by the federal regulators on their web sites, as well as including certain delineations such as the number of times customer notification became necessary as a result of the reported incidences. Statistical information on security breaches is critical; it will significantly improve individuals' ability to evaluate security practices, as currently individuals can only rely upon the vague puffing that appears in GLBA notices.

C. CUSTOMER NOTIFICATION COMPONENT DEMANDS ATTENTION IN CERTAIN AREAS.

The proposed Guidance correctly recognizes that timely notification of customers is important to an institution's reputation. The Guidance appropriately does not to put forth any circumstances that may delay notification of the affected customers. It further establishes that "effective notice may reduce legal risk, assist in maintaining good customer relations, and enable the institution's customers to take steps to protect themselves against the consequences of identity theft."[16] The Guidance does sufficiently address most of the key elements necessary for an effective customer notice.

The proposed Guidance sets forth several optional elements for the customer notice, two of which should be recognized as required elements of the notices. The institutions should be obligated to provide a toll-free telephone number that customers can call to speak to a trained representative that can provide assistance. Also, the institutions should be further bound to offer assistance to the customers in notifying the nationwide credit reporting agencies of the incident and placing a fraud alert in the customers' consumer reports, at no cost to the customers. A security failure on the part of the financial institutions should not commit the customers to treading the waters of correcting consumer credit bureaus' reports alone nor absorb any of the costs associated.

---

[15] *see* Consumer Financial Services Law Report, *Compliance with Safeguard Rule far from Complete*, Vol. 7, No. 5 (August 13, 2003) "...some firms that engage in financial transactions still have not instituted a plan for securing personally identifiable consumer information."

[16] Guidance, appendix, paragraph II.

1. INFORMATION SHOULD BE PROVIDED IN THE NOTICE REGARDING WHAT THE INSTITUTION HAS DONE TO PROTECT THE CUSTOMERS' INFORMATION FROM FURTHER UNAUTHORIZED ACCESS.

An important element of the customer notice overlooked by the proposed Guidance is that the financial institutions should inform affected customers of what the institution has done to protect their information from further unauthorized access. This is essential for customers to make more informed consumer decisions regarding the institution's customer services and whether they are satisfied with the services provided. Moreover, by providing customers notice of the actions taken by the institution, they are more likely to take measures to protect their accounts that may not be redundant nor in disagreement with any of the institution's actions.

2. OFFERING CREDIT COMPANY'S SUBSCRIPTION SERVICES CAN BECOME AN ABUSIVE MARKETING OPPORTUNITY.

The proposed Guidance offers an optional element of informing the customers about subscription services that provide notification anytime there is a request for the customer's credit report.[17] The financial institutions should resist from converting the customer notices into a marketing opportunity for the consumer credit bureaus. While the importance of maintaining vigilance of one's credit security cannot be underscored, especially after an incident involving the unauthorized access to sensitive customer information, the opportunity is too great for possible abusive marketing techniques. The three national bureaus offer different subscription services to monitor credit reporting for instances of fraud that can cost up to $120 per year.[18] Despite the fact that these services may offer helpful information while maintaining the necessary vigilance, offering the service to the customer may mislead the customers into believing that these expensive services are essential. A more cost effective method is to periodically order a credit report, which cost $9.00 each.[19] If the financial institutions are to subscribe the customer to the service, free of charge, the information furnished should not be construed to prefer one service or product to another. Customers can be misled into believing the institution's choice of service is an endorsement for the specific company and its product. If the financial institution is to provide such services, the information should be furnished to the customer on behalf of the institution themselves, preferably on the institution's own letterhead or through the institution's web site.

---

[17] *Id.* at II(D)(3)(b).

[18] Equifax Credit Watch Gold package is offered for $9.95 per month, available at https://www.econsumer.equifax.com/consumer/landing.chtml?^start=&orderSource=EIIW&PP=P3; TransUnion Online Credit Monitoring packages starts at $10.95 per quarter, available at < http://www.transunion.com/Personal/PersonalSolutions.jsp>; and Experian Credit Manager service for $79.95 annually, available at < https://www.creditexpert.com/creditexpert/creditmanager-s/012_1_cm_subscribep3.jsp>.

[19] Equifax Credit Report, $9.00, available at <https://www.econsumer.equifax.com/consumer/landing.ehtml?^start=&orderSource=EHC&PP=P1>.

D. THE STANDARD FOR PROVIDING CUSTOMER NOTICE IS VAGUE.

> *An institution should notify each affected customer when it becomes aware of unauthorized access to sensitive customer information unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur, and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers' accounts for usual or suspicious activity.*[20]

The proposed Guidance warns that an institution may not forgo notifying its customers of an incident because "the institution believes that it may be potentially embarrassed or inconvenienced by doing so."[21] At the outset, each affected customer should be notified every time the financial institution becomes aware of unauthorized access to sensitive customer information. The standard's exception clause to the notification requirement is seriously flawed. It is vague as to what constitutes an "appropriate investigation" which would permit a financial institution to "reasonably" conclude that misuse of the information is unlikely to occur. Financial institutions should be held accountable for their investigative techniques and the conclusions reached with regards to such security incidences. If there are genuine instances misuse is unlikely to occur, the financial institutions should inform their primary Federal regulator of the particulars of their investigation, drawing a conclusion that the customer does not have to be notified of the incident.

The exception clause is further flawed, as the institutions would be required to monitor the affected customers' accounts for unusual or suspicious activity. Unauthorized access to sensitive customer information, and the likelihood for identity theft, can affect a customer's financial integrity beyond the accounts held at the specific financial institution. A financial institution would need either a fraud watch service of one of the national credit bureaus, or a dedicated staff to ensure that the information is not misused in the furtherance of any acts of fraud beyond the customer's accounts with the specific institution. The economic impact on a financial institution for performing effective and comprehensive financial oversight, with the necessary vigilance demanded when dealing with one's credit and financial stability, would far exceed the cost of a customer notification scheme devoid of exceptions.

[20] Guidance, appendix, III.
[21] *Id.* at appendix III(D)(3).

E. THE DEFINITION OF "SENSITIVE CUSTOMER INFORMATION" SHOULD BE BROADENED TO INCLUDE OTHER TYPES OF CUSTOMER INFROMATION.

> *For the purposes of the Guidance, sensitive customer information means a customer's social security number, personal identification number (PIN), password, or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number. It would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such as user name and password.*

The proposed Guidance's definition for "sensitive customer information" above should be broadened to include other information that the financial institutions harbor in their customer information systems to effectively maintain the financial confidence of a customer that is affected by a security incident. Consideration in this definition must be given with regards to customers' account balances, account activity, purchase history, and any investment information. The GLBA places upon financial institutions an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information".[22] The GLBA defines "nonpublic person information" to include personally identifiable financial information resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by the financial institution.[23] The additional information to be added to the definition of sensitive customer information is clearly contemplated by the GLBA. In combination with a personal identifier, the misuse of this information can just as easily result in substantial harm or inconvenience to a customer.

The Electronic Privacy Information Center and the U.S. Public Interest Research Group appreciate this opportunity to present these comments and contribute to the proposed Guidance.

Respectfully Submitted,

Chris Jay Hoofnagle
Associate Director

Edmund Mierzwinski
Consumer Program Director

Munged Dolah
Law Clerk

Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
202-483-1140

U.S. PIRG
218 D St., SE
Washington, DC 20003
202-546-9707

[22] 15 USC § 6801(a).
[23] 15 USC § 6809(4)(A).